International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 2, Apr 2014, 1-4

TRANS STELLAR
• Journal Publications • Research Consultancy

CRYPTOGRAPHY USING ARITHMETIC CODING

MAYURI V. CHAUDHARI[1], VRUSHALI CHOUDHARI[2] & KRANTISH POL[3]

[1,3]Department of Electronics and Telecommunication, B. R. Harne College of Engineering, Karav, Vangani, Ambernath, Thane, Maharashtra, India

[2]Department of Computer Engineering, B. R. Harne College of Engineering, Karav, Vangani, Ambernath, Thane, Maharashtra, India

ABSTRACT

In today's World, both speed of transmission, size of the content with security of data is needed. These criteria can be accomplished by data compression and encryption. Data compression refers to the reduction of the data size while data encryption is to provide more security. By compression of data not only the size of data reduces but also the speed of data transmission increases. Hence, by these techniques you can reduce the data size, increase the data transfer rate and provide security during data transmission.

KEYWORDS: Cryptography, Security of Data, Data Transmission, Arithmetic Coding

INTRODUCTION

Today's communication needs data transmission with more security and less data size. This can be achieved by a system known as compression-crypto system. Compression - crypto system means a system in which both data compression as well as encryption can be achieved simultaneously. Compression is a technique in which data is compressed, eg.zip file and hence, storage space reduces. Thus, the speed of communication increases. Encryption refers to data security where you can use either public key or private key where encryption can be achieved by arithmetic coding.

In data compression, reduction in communication costs can be achieved by using the available bandwidth. Storage space can be reduced by reduction in redundancy in data representation. In the present model-based paradigm for coding an encoded string is produced from input string and a model which is the compressed version of the input. In this way, the encoded string is transferred to the decoder from the encoder. The decoder on the receiver has access to the same model and thus can regenerate the same input string from the encoded string. Also, the decoder must produce exactly the same probability distribution that also in the same context. Greater the complexity of the models, greater is the compression of data. In general, the entropy of a message gives the effectiveness of the model.

Any message needs coding for maintain privacy which can be achieved using Huffman or arithmetic coding. The basic method in Huffman coding is to provide codes of different sizes. Due to this, it creates an ambiguity at the receiver side whether it has reached the last bit or not. Another method known as arithmetic coding can be considered as a generalized form of Huffman coding which represents the occurring sequence with fewer bits.

CRYPTOGRAPHY

Unauthorized access to data, alteration of data, destruction and misappropriate all together have resulted in cryptography. These techniques are very easy to implement and can be decoded easily. In this, the data to be transmitted is

encrypted i.e. encoded by some method using different types algorithms and then transmitted to the receiver side. There are two types of cryptographic schemes:

- Symmetric Key Cryptography
- Asymmetric Key Cryptography

Symmetric Key Cryptography

It is also called as private key cryptography in which a secret key is shared by the sender and the receiver only. Here, the key can be given in advance or can be comprised during transmit.

Asymmetric Key Cryptography

Here, one key is used to encrypt the data and other is used to decrypt it. Hence, it is also known as two-key or public key system. Using this system, not only authentication is main trained but also privacy of the message is attained. But its disadvantage is speed for transmission. Hence, it is combined with traditional key methods.

ARITHMETIC CODING

Arithmetic coding invented by Jorma Rissane is a form of variable length entropy encoding which ensures transmission of lossless data from encoder to decoder. In the other techniques, the message is encrypted by separating it into component symbols and then replacing each symbol by its code word. Conversely, in Arithmetic coding, entire message is encoded into a single number, it operates upon and encodes only one symbol per iteration. Then on each recursion, the symbol is partitioned on number line between 0 and 1 and maintains one of them as a new interval. At the decoder side, magnitude comparison is performed on the code string and the data is regenerated.

Table 1: Probablity Table

Symbol	Probability (%)	Range(Lower, Upper)
#	20	(0.00,0.20)
*	12	(0.20,0.32)
@	15	(0.32,0.37)
.	18	(0.37,0.55)
,	8	(0.55,0.63)
a	2	(0.63,0.65)
e	25	(0.65,0.90)
i	3	(0.90,0.93)
o	6	(0.93,0.99)
u	1	(0.99,1.00)

CONCLUSIONS

In arithmetic coding, a message is encoded as a real number in an interval from one to zero. Arithmetic coding typically has a better compression ratio than Huffman coding, as it produces a single symbol rather than several separate code words. Arithmetic coding is a lossless coding technique. There are a few disadvantages of arithmetic coding. One is that the whole codeword must be received to start decoding the symbols, and if there is a corrupt bit in the codeword, the entire message could become corrupt. Another is that there is a limit to the precision of the number which can be encoded, thus limiting the number of symbols to encode within a codeword. There also exist many patents upon arithmetic coding, so the use of some of the algorithms also call upon royalty fees.

REFERENCES

1. Glen G. Longdon (Jr), "An Introduction to arithmetic coding," *IBM J. RES I 3EVELOP. VOL. 28 NO. 2* MARCH I 984.
2. G. Nigel N. Martin, Glen G. Langdon, Jr., and Stephen J. P. Todd, "Arithmetic Codes for Constrained Channels," *IBM J. Res. Develop.* 27, 94-106 (March 1983).
3. G. G. Langdon, Jr. and J. Rissanen, "A Simple General Binary Source Code," *IEEE Trans. Info. Theory* IT-28, 800-803 (September 1982).
4. Ian H. Willen, Radford M. Neal, And John G. Cleary, "ARITHMETIC CODING FORDATA COIUPRESSION," *Communications of the ACM, June 1987 Volume 30 Number 6*.